Halaman Judul

LAPORAN PENELITIAN

IMPLEMENTASI VIRTUAL PRIVATE NETWORK POINT TO POINT TUNNELING PROTOCOL UNTUK INTEGRASI JARINGAN

oleh
W A G I T O, S.T., M.T.
NIDN : 0522126901
NPP : 961080

Mendapat Bantuan Biaya Penelitian dari Puslitbang dan PPM
Semester Ganjil 2012/2013

Sekolah Tinggi Manajemen Informatika dan Komputer
AKAKOM YOGYAKARTA
Tahun 2013

HALAMAN PENGESAHAN

1.	a. Judul Penelitian	:	Implementasi Virtual Private Network Point To Point Tunneling Protocol Untuk Integrasi Jaringan
	b. Bidang Ilmu	:	Jaringan Komputer
	c. Kategori	:	Implementasi Jaringan Komputer
2.	Ketua Peneliti		
	a. Nama	:	Wagito, S.T., M.T.
	b. NIDN	:	0522126901
	c. NPP	:	961080
	d. Pangkat/Golongan	:	Pembina Tk 1 / IV B
	e. Jabatan Fungsional	:	Lektor Kepala
	f. Jurusan/Prodi	:	Teknik Informatika
	g. Alamat Institusi	:	Jalan Raya Janti Karang Jambe, Yogyakarta
5.	Waktu Penelitian	:	6 bulan
6.	Biaya Penelitian	:	

Yogyakarta, Agustus 2013
Mengetahui

Ketua Prodi

Febri Nova Lenti, S.Si., M.T.
NPP. 961079

Ketua Peneliti

Wagito, S.T., M.T.
NPP. 961080

Menyetujui

Kepala Puslitbang dan PPM
STMIK AKAKOM

Dra. Syamsu Windarti, M.T., Apt
NIP. 19660710 199303 2 001

Kata Pengantar

Puji syukur saya panjatkan ke hadirat Allah S.W.T. karena hanya dengan rahmat dan hidayah-Nya. Berkat pertolongan dan tuntunan-Nya serta dengan berbagai usaha akhirnya penelitian ini berhasil diselesaikan dengan baik.

Penelitian yang berjudul Implementasi *Virtual Private Network Point To Point Tunneling Protocol* Untuk Integrasi Jaringan ini dikembangkan dengan tujuan untuk membuat konfigurasi perangkat keras dan perangkat lunak untuk difungsikan dalam integrasi dua jaringan. Dua jaringan yang dilakukan integrasi adalah jaringan pondok pesantren Ibnul Qoyyim putra dan putri. Penelitian memanfaatkan router RB750 sebagai router jaringan Internet dan Mikrotik RouterOS™ sebagai perangkat lunak untuk mengelola tabel *routing*, *Firewall* dan protokol PPTP.

Penulis menyadari bahwa hasil penelitian ini masih banyak kekurangannya, sehingga kritik dan saran yang membangun untuk lebih mengembangkan hasilnya sangat diharapkan. Semoga hasil penelitian ini bermanfaat bagi pengembangan ilmu pengetahuan dan teknologi.

Penulis

Daftar Isi

Daftar Gambar

ABSTRAK

Jaringan komputer sudah menjadi kebutuhan sangat penting bagi institusi yang menerapkan pengolahan data berbasis komputer. Ukuran jaringan komputer yang diperlukan sangat tergantung pada besar atau kecilnya institusi. Institusi yang kecil mungkin cukup menggunakan jaringan komputer yang sederhana. Institusi yang punya tempat yang luas dan terdiri dari beberapa lokasi, memerlukan jaringan komputer yang luas. Apabila masih dalam jangkauan jaringan kabel, antar lokasi pada institusi tersebut dapat dihubungkan secara mudah.

Suatu masalah timbul untuk mengintegrasikan jaringan apabila antar lokasi pada institusi letaknya cukup jauh. Apabila dua lokasi masih dapat dijangkau oleh jaringan, maka permasalahan dapat diatasi. Permasalahan semakin terlihat, apabila institusi punya beberapa lokasi yang berjarak sangat jauh sedemikian, sehingga jaringan *wireless* tidak dapat digunakan. Untuk mengatasi masalah ini, usulan teknik yang dapat digunakan adalah VPN menggunakan protokol tertentu untuk mengintegrasikan dua jaringan. Salah satu protokol yang dipakai dalam VPN adalah PPTP.

Tujuan yang ingin dicapai dari hasil penelitian yang dilakukan adalah membuat prototipe konfigurasi perangkat keras dan perangkat lunak untuk integrasi jaringan pada tingkat laboratorium, menerapkan integrasi jaringan pada pondok pesantren Ibnul Qoyyim putra dan putri, memanfaatkan *router* RB750 sebagai *router* jaringan Internet dan mempermudah pertukaran data antar jaringan.

Kata kunci: integrasi, jaringan, VPN, PPTP

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer sudah menjadi kebutuhan sangat penting bagi institusi yang menerapkan pengolahan data berbasis komputer. Semua data yang berkaitan dengan institusi tersebut disimpan dalam komputer. Semua kegiatan yang berkaitan dengan transaksi harian institusi didasarkan pada data tersebut. Kebutuhan jaringan komputer semakin terasa apabila data diletakkan pada komputer-komputer yang berbeda. Keberadaan jaringan komputer sangat membantu dalam proses penyampaian data dari suatu komputer ke komputer lain.

Ukuran jaringan komputer yang diperlukan sangat tergantung pada besar atau kecilnya institusi. Institusi yang kecil mungkin cukup menggunakan jaringan komputer yang sederhana. Institusi yang punya tempat yang kecil, tentunya hanya memerlukan jaringan komputer yang kecil. Institusi yang punya tempat yang luas dan terdiri dari beberapa lokasi, memerlukan jaringan komputer yang lebih luas. Apabila masih dalam jangkauan jaringan kabel, antar lokasi pada institusi tersebut dapat dihubungkan secara mudah.

Suatu masalah timbul apabila antar lokasi pada institusi letaknya cukup jauh. Apabila jarak lokasi institusi sudah di luar jangkau jaringan kabel, jaringan

wireless dapat dipakai untuk menyatukan lokasi-lokasi tersebut. Jaringan *wireless* punya jangkau yang lebih jauh dibanding jaringan kabel, namun punya keterbatasan jarak jangkau. Penggunaan jaringan *wireless* juga memerlukan investasi untuk membeli peralatan dan sarana pemasangan jaringan *wireless*. Penggunaan jaringan *wireless* juga memerlukan suatu lokasi yang tidak terhalang antar lokasinya.

Permasalahan semakin terlihat, apabila institusi punya beberapa lokasi yang berjarak sangat jauh. Misalnya, jaraknya berada di luar jangkau jaringan *wireless*. Atau lokasi-lokasi institusi tersebut terpisah oleh daerah yang punya halangan geografis, sehingga pemasangan sarana *wireless* tidak dimungkinkan.

Pada saat ini jaringan Internet punya penggunaan yang sangat luas. Penggunaan jaringan Internet bagi institusi umumnya hanya sekadar mengakses halaman situs, mengirim *e-mail*, melakukan *chat* atau melakukan komunikasi pada media sosial. Bagi institusi tertentu, jaringan Internet hanya merupakan fasilitas sarana hiburan. Namun bagi institusi lain, Internet menjadi tulang punggung bagi kelancaran kegiatannya atau bahkan menjadi sarana menghasilkan keuntungan.

Jaringan Internet juga dapat digunakan untuk menghubungkan institusi yang letaknya sangat jauh. Menghubungkan beberapa lokasi institusi yang sangat jauh harus menjamin keamanan data yang dikirimkan.

Salah satu kemampuan jaringan komputer adalah membuat suatu VPN (*Virtual Private Network*). VPN tidak sekadar menghubungkan dua lokasi yang

sangat jauh, namun punya kemampuan untuk menyembunyikan data yang dikirimkan. VPN dapat dilewatkan pada suatu jaringan publik seperti Internet. VPN membuat semacam saluran rahasia (*tunnel*) melintasi jaringan publik.

Ada beberapa protokol untuk menerapkan VPN, salah satunya adalah PPTP (*Point-to-Point Tunneling Protocol*). PPTP adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari klien yang terpisah jauh kepada *server* dengan cara membuat VPN melalui jaringan data berbasis TCP/IP.

Jaringan Internet beroperasi menggunakan banyak protokol. Untuk mengakses halaman situs digunakan protokol HTTP, untuk mengirim *e-mail* digunakan protokol SMTP, untuk mengirim *file* digunakan protokol FTP, dan sebagainya. Jaringan Internet dapat dimanfaatkan untuk menghubungkan institusi yang terpisah jauh.

Teknologi VPN memungkinkan untuk dibangun suatu integrasi antar dua sistem jaringan yang yang ada pada Pondok Pesantren IBNUL QOYYIM. Pondok pesantren mengelola dua lokasi yang terpisah, masing-masing untuk santri putri dan santri putra.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian adalah bagaimana mengintegrasikan dua jaringan yang terpisah menggunakan teknologi VPN dengan PPTP.

1.3 Batasan Masalah

Batasan yang perlu diperhatikan dalam kaitan dengan kemungkinan masalah yang muncul penelitian adalah:

- penelitian dititikberatkan pada penentuan metode untuk melakukan integrasi jaringan,
- jaringan terpisah oleh lokasi yang sangat jauh,
- menggunakan jaringan publik untuk sarana jalur integrasi, dan
- tidak membicarakan keamanan akibat pemanfaatan jaringan publik untuk integrasi jaringan.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari hasil penelitian yang dilakukan adalah sebagai berikut.

- Membuat prototipe konfigurasi perangkat keras dan perangkat lunak untuk integrasi jaringan pada tingkat laboratorium.
- Menerapkan integrasi jaringan pada pondok pesantren Ibnul Qoyyim putra dan putri
- Memanfaatkan *router* RB750 sebagai *router* jaringan Internet untuk integrasi jaringan.
- Mempermudah pertukaran data antar jaringan menggunakan *share*, memperpendek jalur, koneksi HTTP dan koneksi basisdata.

1.5 Manfaat Penelitian

Manfaat penelitian adalah bahwa hasilnya dapat diterapkan untuk membuat integrasi jaringan institusi yang punya lokasi terpisah. Penerapan dapat memanfaatkan penyedia jaringan Internet yang dapat memberi fasilitas IP publik pada pelanggan.

1.6 Target Luaran

Luaran yang ditargetkan pada penelitian ini adalah berupa metode untuk mengintegrasikan jaringan terpisah lokasi yang sangat jauh. Hasil penelitian direncanakan dilakukan publikasi dan seminasi pada kegiatan ilmiah. Kegiatan ilmiah yang diharapkan bisa diikuti adalah seminar nasional *Open Source Software* (OSS) yang diselenggarakan LIPI.

BAB 2 TINJAUAN PUSTAKA

Beberapa penelitian berkaitan dengan integrasi jaringan komputer pernah dilakukan. Beberapa penelitian berkaitan dengan integrasi jaringan yang pernah dilakukan antara lain sebagai berikut.

Pada studi kasus yang dilakukan oleh Nova Rusydi Setyawan pada tahun 2011 dengan judul "Implementasi VLAN *Trunk Protocol* (VTP) melalui *Ethernet over Internet Protocol* (EoIP) *Tunnel* pada Mikrotik RouterOS" membahas penggunaan *Ethernet over Internet Protocol* pada sistem operasi Mikrotik RouterOS untuk melewatkan VLAN Trunk Protocol. Protokol yang dipakai adalah EoIP yang merupakan salah satu bentuk protokol *tunneling*.

Protokol EoIP memungkinkan pembentukan saluran khusus (tunnel) Ethernet antara dua *router* di atas hubungan IP. Antarmuka EoIP muncul di atas antarmuka Ethernet. Pada penelitian dilakukan kombinasi dengan fitur VLAN untuk konfigurasi jaringan dengan memanfaatkan Mikrotik RouterOS™ sebagai peralatan utama. Fitur VLAN hanya mempermudah dalam konfigurasi jaringan.

Penelitian Dedy Cahyadi program studi Ilmu Komputer 2010, FMIPA Universitas Mulawarman dengan judul "Pemanfaatan Fitur *Tunneling* Menggunakan *Virtual Interface* EoIP di Mikrotik RouterOS untuk koneksi *Bridging* Antar Kantor Melalui Jaringan ADSL Telkom Speedy" yang membahas

tentang pemanfaatan koneksi EoIP dengan Mikrotik RouterOS untuk Integrasi antar kantor melalui jaringan ADSL Telkom Speedy, sehingga jaringan antar kantor menjadi satu jaringan.

Salah satu fitur yang bisa dikembangkan dari protokol EoIP adalah pembentukan jembatan *bridge*. Ketika fungsi *bridge* pada router diaktifkan, semua lalu-lintas Ethernet (protokol Ethernet) akan dilewatkan pada *bridge*. *Bridge* berlaku seperti antarmuka dan kabel fisik Ethernet antara dua *router*. Sebagai saluran publik, pada penelitian ini digunakan jaringan *broadband* ADSL Telkom Speedy.

Penelitian dari Nanda Pramudya, Universitas Duta Wacana tahun 2009 tentang "Implementasi dan Analisis *Point-to-Point Tunneling Protocol* Serta Ethernet Over Internet Protocol Sebagai Metode Untuk Membuat *Virtual Private Network*" yang membahas tentang implementasi dan analisis *Point-to-Point Tunneling Protocol* dan *Ethernet Over Internet Protocol* digunakan sebagai VPN.

Pada penelitian ini juga dimanfaatkan protokol EoIP untuk integrasi jaringan. Sebagai saluran digunakan protokol PPTP. Dengan demikian, pada penelitian ini menggabungkan protokol VPN PPTP dengan protokol EoIP. Namun pada penelitian ini tidak mengaktifkan fitur *bridge*.

Penelitian Kukuh Prasetyo dari Institut Teknologi TELKOM tentang "Analisis Performasi Pada Penggunaan IPsec dan PPTP Untuk *Internet Protocol Television* (IPTV)" yang membahas perbandingan di antara ke dua protokol IPsec dan PPTP dengan parameter yang dibandingkan dan diuji yaitu : pengaruh

autentikasi, enkripsi dan enkapsulasi yang berbeda diantara dua protokol tersebut terhadap IPTV.

Penelitian tersebut membandingkan penggunaan protokol PPTP dan IPsec (IP *secure*). Protokol PPTP sebetulnya sudah menentukan sebagai saluran khusus untuk integrasi jaringan. IPsec dapat diaktifkan pada Mikrotik RouterOS™. Secara bawaan fitur ini tidak aktif. Implementasi diuji pengaruhnya terhadap IPTV. Penggunaan IPsec pada satu sisi bisa digunakan untuk meningkatkan keamanan, namun pada sisi lain akan menambah beban pekerjaan *router*. Dal hal ini bisa saja memengaruhi kinerja sistem jaringan.

Pemanfaatan VLAN hanya memudahkan dalam konfigurasi jaringan namun sebetulnya menurunkan kinerja jaringan. Sebetulnya VLAN secara dasar sistem operasi hanya memanfaatkan kemampuan IP alias pada satu antarmuka fisik. IP alias berupa antarmuka virtual. Dengan demikian VPN sebetulnya cukup membebani kerja router.

Protokol EoIP memungkinkan pembentukan saluran khusus (*tunnel*) Ethernet antara dua router di atas hubungan IP. Antarmuka EoIP muncul di atas antarmuka Ethernet. Protokol PPTP memungkinkan pembentukan saluran pada integrasi jaringan. Apabila protokol EoIP digabungkan dengan protokol PPTP, maka yang terjadi adalah pembentukan saluran di dalam saluran. Hal demikian mungkin meningkatkan keamanan, namun jelas membebani router.

Pada penelitian “Implementasi VPN PPTP Untuk Integrasi Jaringan” dicoba dirancang integrasi dua jaringan dengan hanya memanfaatkan protokol

PPTP. Dengan metode ini, diharapkan beban *router* menjadi lebih ringan, sedemikian sehingga kecepatan transmisi data tidak terlalu terpengaruh. Untuk keperluan pengarahan paket data dimanfaatkan metode *routing* statis. Metode *routing* statis pada satu sisi agak sedikit lebih sulit diterapkan, namun lebih cepat dan lebih stabil dalam menangani proses *routing*. Metode ini digunakan untuk integrasi dua jaringan terpisah yaitu jaringan pada pondok pesantren Ibnul Qoyyim putra dan putri.

BAB 3 TEORI

3.1 Alamat IP

Alamat IP di Internet dikelola oleh APNIC (*Asia Pasific Network Information Center*) untuk kawasan Asia Pasific. APNIC memiliki tugas membagi blok Nomor IP dan Nomor AS (*Automous System*) kepada para ISP pada kawasan Asia Pasific. Selain itu juga mengelola *authoritive registration server* (whois) dan *reverse domains* (in-addr.arpa). (Angga Wibowo, 2006)

Alamat IP (versi 4) umumnya dalam bentuk 4 bilangan desimal yang masing-masing dipisahkan oleh sebuah titik. Setiap bilangan desimal tersebut merupakan nilai dari satu *octet* (delapan bit) alamat IP.

IPv4 terbagi atas tiga kelas yaitu kelas A, kelas B dan kelas C. Jumlah alamat jaringan yang dimungkinkan pada masing-masing kelas adalah sebagai berikut.

- Kelas A: 128
- Kelas B: 16.384
- Kelas C: 2.097.152

Jumlah alamat IP untuk *host* yang dimungkinkan pada masing-masing

kelas adalah sebagai berikut.

- Kelas A: 16.777.214
- Kelas B: 65.534
- Kelas C: 254

Untuk memisahkan *network id* dan *host id* digunakan *netmask* (*default*) dengan mendefinisikan bagian *network id* dinyatakan dengan angka biner 1, sedangkan *host id* dinyatakan dengan angka biner 0. *Netmask* ini biasanya disertakan pada nomor IP dalam bentuk prefiks *network* yaitu jumlah angka biner 1 pada *network id*. (rizqtech, 2009)

3.2 Sub Network

Proses untuk memecah sebuah jaringan dengan jumlah *host* yang cukup banyak, menjadi beberapa jaringan dengan jumlah *host* yang lebih sedikit disebut *sub netting*. Secara mudah *sub netting* dapat dikatakan sebagai proses pembentukan *sub network*. Adapun kegunaan dari *sub netting* adalah sebagai berikut.

- Untuk menentukan batas *network* ID dalam suatu *subnet*.
- Memperbanyak jumlah *network* (LAN).
- Mengurangi jumlah *host* dalam satu *network*.
- Untuk mengurangi tingkat kongesti (gangguan/tabrakan) lalulintas data dalam suatu *network*.

Perhitungan *sub netting* bisa dilakukan dengan dua cara yaitu biner dan khusus. Penulisan alamat alamat IP umumnya adalah dengan 192.168.1.2. Namun adakalanya ditulis dengan 192.168.1.2/24. Penjelasan tentang hal ini adalah bahwa alamat IP 192.168.1.2 dengan *subnet mask* 255.255.255.0. Maksud /24 diambil dari perhitungan bahwa 24 bit *subnet mask* diselubungi dengan biner 1 atau sama dengan 11111111.11111111.11111111.00000000 (255.255.255.0). (lesta_bd, 2011)

3.3 VLAN

VLAN (*Virtual Local Area Network*) adalah pengelompokan *logical host-host* yang terhubung pada *port-port* yang telah ditentukan secara administratif pada sebuah *switch*. Dengan menggunakan VLAN ini maka manajemen *network* akan menjadi semakin sederhana. Beberapa cara VLAN menyederhanakan manajemen *network* adalah

- Perubahan *network* dilakukan dengan melakukan konfigurasi *port* pada *switch* ke VLAN yang sesuai.
- Pembatasan hak akses pengguna dilakukan dengan mengelompokkan *host* dalam sebuah VLAN yang terkena isolasi.
- VLAN menjadikan *host* tidak tergantung terhadap lokasi fisik maupun geografis.
- VLAN-VLAN dapat meningkatkan jumlah *broadcast* domain dan pada

saat yang sama memperkecil ukuran *broadcast* domain itu sendiri.

VLAN pada Mikrotik RouterOS™ dapat dibuat dengan menempatkan VLAN tersebut di bawah antarmuka lain sebagai induknya, misalnya antarmuka Ethernet. Antarmuka induk tersebut bisa difungsikan hanya sebagai induk dari VLAN-VLAN. (Cakrawala21.com, 2011)

3.4 EoIP

Ethernet over Internet Protocol (EoIP) adalah protokol pada Mikrotik RouterOS yang menciptakan sebuah *tunnel* Ethernet antara dua buah *router* yang mana *tunnel* tersebut berada di atas IP. *Tunnel* EoIP dapat berjalan pada dua buah *tunnel* lain yaitu *tunnel* IPIP, *tunnel* PPTP atau *tunnel* yang lain yang berbasis IP. (www.kuebasah.com, 2008). Dalam hal ini, antarmuka EoIP muncul di atas antarmuka Ethernet

Salah satu fitur yang bisa dikembangkan dari protokol EoIP adalah pembentukan jembatan *bridge*. Ketika fungsi *bridge* pada router diaktifkan, semua lalu-lintas Ethernet (protokol Ethernet) akan dilewatkan pada *bridge*. *Bridge* berlaku seperti antarmuka dan kabel fisik Ethernet antara dua *router*.

3.5 PPTP

Point-to-Point Tunneling Protocol adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari *remote client* kepada *server*

perusahaan swasta dengan membuat suatu VPN melalui jaringan data berbasis TCP/IP. Teknologi jaringan PPTP merupakan perluasan dari *remote access Point-to-Point protocol* . PPTP adalah suatu protokol jaringan yang membungkus paket PPP ke dalam IP *datagram* untuk transmisi yang dilakukan melalui Internet atau jaringan publik berbasis TCP/IP. PPTP dapat juga digunakan pada jaringan *LAN-to-LAN*.

Fitur penting dalam penggunaan PPTP adalah dukungan terhadap VPN dengan menggunakan *Public Switched Telephone Network* (PSTN). PPTP menyederhanakan dan mengurangi biaya dalam penggunaan pada perusahaan besar dan sebagai solusi untuk *remote* atau *mobile users* karena PPTP memberikan komunikasi yang aman dan dienkripsi melalui *line public telephone* dan Internet.

Secara umum, terdapat tiga komponen di dalam komputer yang menggunakan PPTP yaitu (Margaret Rouse, 2005) :

- PPTP *client*
- Network Access Server
- PPTP *server*

3.6 Mikrotik

Mikrotik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP *network* dan jaringan *wireless*. Sistem operasi Mikrotik RouterOS™ cocok digunakan oleh ISP dan

provider hotspot.

Fitur-fitur Mikrotik sangat banyak. Fitur Mikrotik yang berkaitan dengan protokol TCP/IP antara lain *Firewall* dan NAT, *routing* statis dan *routing* dinamis, *Data Rate Management*, *Hotspot*, *Point-to-Point tunneling protocol*, *Simple tunnel*, IPsec. *Web proxy*, *Caching* DNS *client*, DHCP, *Universal Client*, VRRP, UPNP, NTP, *Monitoring/Accounting*, SNMP, M3P, MNDP, *Tools* dan sebagainya. Fitur Mikrotik yang berkaitan dengan konektivitas antara lain *wireless*, *Bridge*, *Virtual* LAN, *Synchronous*, *Asynchronous*, ISDN, SDSL dan sebagainya (Mikrotik, 2008).

Mikrotik RouterOS™ hadir dalam berbagai *level* kemampuan. Tiap *level* memiliki kemampuannya masing-masing, mulai dari *level* 3, hingga *level* 6. Secara singkat, *level* 3 digunakan untuk *router* yang punya antarmuka Ethernet, *level* 4 untuk klien *wireless* atau serial antarmuka, *level* 5 untuk *wireless* AP, dan *level* 6 tidak mempunyai limitasi apa pun. Untuk aplikasi *hotspot*, bisa digunakan *level* 4 (200 pengguna), *level* 5 (500 pengguna) dan *level* 6 (tidak terbatas).

3.7 Winbox

Konfigurasi Mikrotik RouterOS™ dapat dilakukan dengan dua cara yaitu: melakukan *login* ke *server* Mikrotik menggunakan utilitas Telnet atau SSH dan menggunakan utilitas Winbox. Konfigurasi dengan cara *login* ke *server* Mikrotik dilakukan dengan cara memberi perintah-perintah tertentu dari *shell* Mikrotik. Konfigurasi dengan cara ini cukup sulit bagi pengguna pemula. Winbox

merupakan utilitas yang disediakan Mikrotik untuk menangani konfigurasi secara visual.

Semua pengaturan Mikrotik hampir seluruhnya disediakan secara visual oleh Winbox. Utilitas Winbox menyediakan banyak menu antara lain *Interfaces*, *Wireless*, *Bridge*, *Mesh*, PPP, IP, *Routing*, *Port*, *System*, Terminal dan sebagainya. Menu penting yang berkaitan dengan penelitian ini adalah IP *Address* dan IP *Routes*. Menu IP *Address* berkaitan dengan pemberian alamat IP pada antarmuka *router*. IP *Routes* berkaitan dengan penyusunan tabel *routing* pada *router*.

Selain itu, Winbox juga menyediakan terminal untuk melakukan konfigurasi menggunakan *shell* dan pengaturan lain yang belum disediakan pada fasilitas visual. Salah satu fasilitas yang membuat Winbox sangat fleksibel adalah ketersediaan pembuatan sekrip program. Dengan sekrip ini, Mikrotik RouterOS™ dapat dikendalikan secara terprogram.

BAB 4 METODE PENELITIAN

4.1 Bahan Penelitian

Bahan yang digunakan dalam penelitian Mikrotik RouterOS™, *router* RB750, jaringan komputer laboratorium STMIK Akakom dan jaringan pondok pesantren Ibnul Qoyyim. Pengaruh integrasi jaringan diamati pada beberapa aplikasi jaringan lapis empat TCP/IP yaitu layanan *share* data, layanan HTTP, layanan MySQL dan layanan transfer *file*.

4.2 Alat

Alat yang digunakan dalam penelitian ini berupa perangkat keras dan perangkat lunak. Perangkat lunak yang digunakan dalam penelitian adalah sebagai berikut.

- Sistem Operasi Mikrotik RouterOS™.
- Sistem Operasi Windows.
- Sistem Operasi Linux.
- Web Browser Mozilla.
- tracert.
- traceroute.

- ping.

Perangkat keras yang digunakan dalam penelitian umumnya adalah perangkat keras jaringan komputer yang meliputi sebagai berikut.

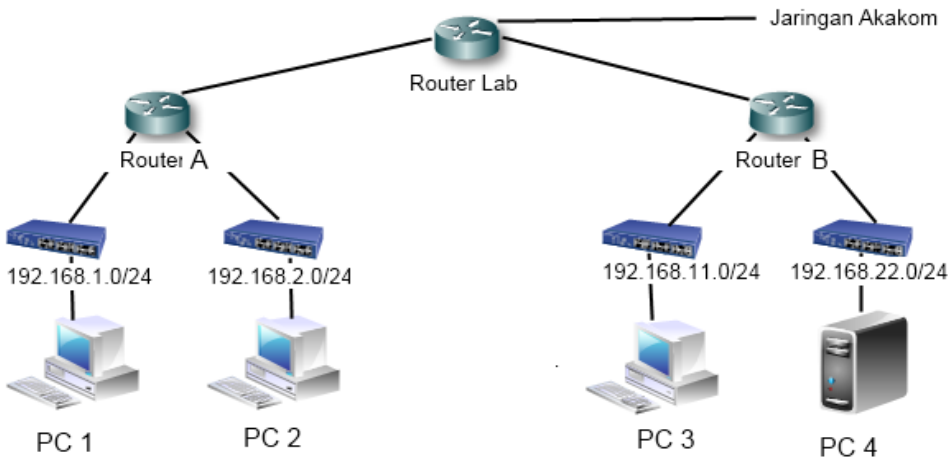
- *switch* RB250GS.
- *router* RB750.
- PC/*laptop*.
- kabel UTP *straight.*
- kabel UTP *cross link.*
- LAN *tester*.
- konektor RJ-45.
- *crimping Tools*.

4.3 Jalan Penelitian

Penelitian dilakukan dalam dua tahap yaitu penelitian pada tingkat laboratorium dan penelitian di lapangan. Penelitian di laboratorium dimaksudkan untuk membuat dan meneliti konfigurasi sebelum diterapkan di lapangan. Penelitian di lapangan dimaksudkan untuk menerapkan hasil uji coba yang sudah dilakukan di laboratorium.

4.3.1 Rancangan Laboratorium

Konfigurasi jaringan yang diterapkan di laboratorium diusahakan mirip dengan konfigurasi yang diterapkan di lapangan. Titik berat penerapan jaringan terletak pada bagian integrasi jaringan. Konfigurasi perangkat keras jaringan komputer yang diterapkan di laboratorium dapat digambarkan pada Gambar 4.1 sebagai berikut.



Gambar 4.1 Diagram Jaringan Tingkat Laboratorium

penjelasan konfigurasi perangkat keras:

- Jaringan lokal A menggambarkan jaringan yang diterapkan pada pondok pesantren putra Ibnul Qoyyim, sedangkan jaringan lokal B menggambarkan jaringan yang diterapkan pada pondok pesantren putri Ibnul Qoyyim.
- *Router* pada pondok pesantren putra diwakili oleh *router* A, sedangkan

router pada pondok pesantren putri diwakili oleh *router* B.

- Seluruh sistem pemasangan kabel pada pondok pesantren putra diwakili oleh satu switch A, sedangkan sistem pemasangan kabel pada pondok pesantren putri diwakili oleh switch B.
- Komputer PC1 dan PC2 mewakili komputer-komputer yang ada pada dua pondok pesantren putra, sedangkan komputer PC3 dan PC4 mewakili komputer-komputer pada pondok pesantren putri.
- Kedua sistem jaringan dihubungkan menggunakan EoIP dan PPTP melalui jaringan laboratorium.
- Jaringan laboratorium mewakili jaringan publik (Internet) yang diterapkan. Hubungan jaringan (baik jaringan A maupun B) menuju jaringan laboratorium menggunakan *Firewall*.
- Mesin yang difungsikan sebagai *Firewall* pada jaringan adalah adalah *router*.
- Alamat IP publik yang harus diterapkan pada *Firewall* digunakan alamat IP privat milik laboratorium.

Langkah-langkah konfigurasi VPN PPTP.

Membangun Hubungan VPN PPTP

- Pengaturan pada jaringan A
  - diatur alamat IP pada komputer PC1 dan PC2
  - diatur alamat *default gateway* komputer PC1 dan PC2

- diatur alamat IP antarmuka *router* A yang menuju jaringan publik
- diatur alamat IP semua antarmuka *router* A yang menghadap jaringan privat
- diatur *Network Address Translation* (NAT) pada *router* A
- diuji koneksi jaringan A dari PC1 dan PC2

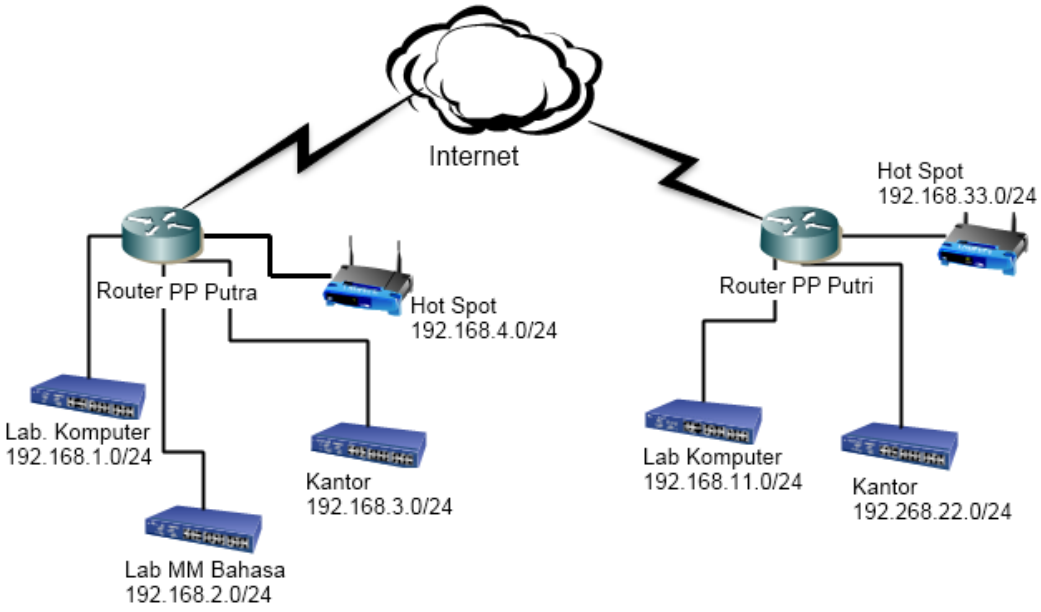
- Pengaturan pada jaringan B
  - diatur alamat IP pada komputer PC3 dan PC4
  - diatur alamat *default gateway* komputer PC3 dan PC4
  - diatur alamat IP antarmuka *router* B yang menuju jaringan publik
  - diatur alamat IP semua antarmuka *router* B yang menghadap jaringan privat
  - diatur *Network Address Translation* (NAT) pada *router* B
  - diuji koneksi jaringan B dari PC3 dan PC4

- Menghubungkan *router* A dan *router* B
  - disiapkan *server* PPTP pada *router* A
  - disiapkan klien PPTP pada *router* B

- Membentuk tabel *routing*
  - diatur tabel *routing* pada *router* A
  - diatur tabel *routing* pada *router* A

4.3.2 Rancangan Lapangan

Rancangan integrasi jaringan PPIQ Putra dan Putri didasarkan pada hasil rancangan simulasi di laboratorium. Model jaringan komputer pada dua pondok pesantren tersebut dapat dilihat pada Gambar 4.2. Jaringan lokal PPIQ Putra dan Putri masing-masing terhubung pada jaringan Internet.



Gambar 4.2 Diagram Integrasi PPIQ Putra dan Putri

Router PP Putra bertugas untuk melayani kebutuhan jaringan pada seluruh komputer pada jaringan pondok pesantren putra, sedangkan *router* PP Putri melakukan hal yang sama untuk pondok pesantren putri. Kebutuhan jaringan

terutama layanan pemberian alamat IP, *server* DNS dan *Gateway* pada komputer. Kebutuhan tersebut dilayani *router* melalui layanan *server* DHCP. Selain itu, *router* berfungsi juga sebagai *Firewall* bagi masing-masing jaringan.

Router PP Putra dan Putri dihubungkan menggunakan metode VPN PPTP. Metode ini merupakan hubungan Point-to-Point antara *server* dan klien PPTP. *Router* PP Putra dikonfigurasi sebagai *server* PPTP, sedangkan *router* PP Putri dikonfigurasi sebagai klien PPTP. Sebagai *server* PPTP, *router* PP Putra harus menggunakan alamat IP publik supaya dapat diakses dari luar. Sebagai klien PPTP, *router* PP Putri tidak perlu menggunakan alamat IP publik karena klien bertugas untuk aktif menghubungi *server*.

BAB 5 IMPLEMENTASI DAN PEMBAHASAN

5.1 Implementasi

Tahap implementasi dilakukan dengan melakukan konfigurasi pada seluruh *router* dan komputer yang terdapat dalam sistem jaringan. *Router* yang terlibat dalam sistem jaringan meliputi *router* A yang mewakili *router* pada PP putra dan *router* B yang mewakili *router* pada PP putri Ibnul Qoyyim.

5.1.1 Implementasi Pada Laboratorium

Pengaturan Pada Jaringan A

Konfigurasi awal *router* A meliputi alamat IP dan NAT. Antarmuka pada *router* A ada tiga yaitu ether1, ether2 dan ether3. Antarmuka ether1 merupakan antarmuka *router* yang menghadap jaringan publik. Alamat IP antarmuka ether1 mengikuti alamat IP yang diberikan oleh jaringan laboratorium menggunakan protokol DHCP. Dengan demikian antarmuka ether1 dikonfigurasi sebagai klien DHCP.

```
[admin@MikroTik] > ip dhcp-client add interface=ether1
[admin@MikroTik] > ip dhcp-client enable numbers=0
```

Alamat IP yang diperoleh antarmuka ether1 dari *server* DHCP

laboratorium Periferal STMIK AKAKOM adalah 172.18.105.104/26. Alamat IP ini merupakan alamat IP dinamis. Dalam percobaan tingkat laboratorium diperlakukan seperti alamat IP publik.

Antarmuka ether2 dan ether3 diberi alamat IP yang satu jaringan dengan jaringan yang menjadi tanggung jawabnya. Antarmuka ether2 diberi alamat IP 192.168.1.1/24, sedangkan antarmuka ether2 diberi alamat IP 192.168.2.1/24.

```
[admin@MikroTik] > ip address add interface=ether2
address=192.168.1.1/24
[admin@MikroTik] > ip address add interface=ether3
address=192.168.2.1/24
```

Hasil konfigurasi alamat IP antarmuka pada *router* A dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 172.18.105.61/26   172.18.105.0    ether1
 1   192.168.1.1/24     192.168.1.0     ether2
 2   192.168.2.1/24     192.168.2.0     ether3
```

Setelah alamat IP pada antarmuka *router* dikonfigurasi, tabel *routing* yang berkaitan dengan jaringan yang menjadi tanggung jawab *router* secara otomatis akan dibentuk oleh *router*. Tabel *routing* yang otomatis terbentuk dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.62   1
 1 ADC  172.18.105.64/26  172.18.105.61   ether1          0
 2 ADC  192.168.1.0/24    192.168.1.1     ether2          0
```

```
 3 ADC  192.168.2.0/24    192.168.2.1     ether3          0
```

Tabel *routing* yang yang otomatis terbentuk setelah *router* diberi alamat IP diberi kode ADC yang merupakan singkatan dari *active dynamic connect*. Arti kode ADC adalah bahwa jaringan tersebut aktif, dihasilkan secara otomatis dan dalam kondisi terhubung. Pada tabel *routing* juga terdapat kode ADS yang merupakan singkatan dari *active dynamic static*. Kode ini diberikan pada tabel *routing* yang berkaitan dengan *default route* pada *router*. *Default route* pada *router* A adalah 172.18.105.126 yang diperoleh secara otomatis dari *router* laboratorium menggunakan protokol DHCP.

Pada *router* A perlu dikonfigurasi aturan yang berkaitan dengan rantai NAT. Dalam kasus ini, *router* menjalankan fungsi sebagai *Firewall*. Mesin *Firewall* melakukan proses NAT terhadap paket data yang berasal dari jaringan 192.168.1.0/24 dan jaringan 192.168.2.0/24. Pada penelitian ini digunakan salah satu bentuk NAT yang disebut *masquerade*. *Masquerade* sesuai diterapkan untuk proses NAT pada antarmuka yang punya alamat IP dinamis.

```
[admin@MikroTik] > ip firewall nat add chain=srcnat
action=masquerade out-interface=ether1 src-address=192.168.1.0/24
[admin@MikroTik] > ip firewall nat add chain=srcnat
action=masquerade out-interface=ether1 src-address=192.168.2.0/24
```

Hasil konfigurasi aturan rantai *Firewall* yang diterapkan pada *router* dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade src-address=192.168.1.0/24
```

```
out-interface=ether1
 1   chain=srcnat action=masquerade src-address=192.168.2.0/24
out-interface=ether1
```

Tampilan aturan rantai *Firewall* tersebut menunjukkan bahwa paket data yang berasal dari jaringan 192.168.1.0/24 yang keluar melalui antarmuka ether1 dikenakan proses *masquerade*. Demikian juga paket data yang berasal dari jaringan 192.168.2.0/24 yang keluar melalui antarmuka ether1 dikenakan proses *masquerade*.

Sampai pada tahap ini, konfigurasi alamat IP dan aturan NAT pada *router* A sudah cukup. Selanjutnya, konfigurasi dilakukan pada seluruh komputer klien yang menjadi tanggung jawab *router* A.

Konfigurasi pada komputer klien meliputi alamat IP, alamat IP *server* DNS dan *default gateway*. Pengaturan tiga hal ini dilakukan secara dinamis menggunakan protokol DHCP. Alasan penggunaan protokol DHCP untuk memberi alamat IP pada komputer klien karena jumlah komputer klien yang banyak. Protokol DHCP memungkinkan pengaturan tiga parameter jaringan tersebut secara terpusat. Dalam kaitan ini, *router* berlaku sebagai *server* DHCP.

Pengaturan *server* DHCP pada *router* A meliputi pengaturan *pool* alamat IP yang akan diberikan kepada komputer klien, pengaturan alamat *server* DNS dan *default gateway* tiap-tiap jaringan. Pengaturan *pool* alamat IP komputer klien dapat dilakukan sebagai berikut.

```
[admin@MikroTik] > ip pool add name=pool1 ranges=192.168.1.2-
192.168.1.254
[admin@MikroTik] > ip pool add name=pool2 ranges=192.168.2.2-
```

```
192.168.2.254
```

Hasil pengaturan *pool* alamat IP dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip pool print
 # NAME                RANGES
 0 pool1               192.168.1.2-192.168.1.254
 1 pool2               192.168.2.2-192.168.2.254
```

Router A punya tanggung jawab untuk mengelola dua jaringan yaitu jaringan 192.168.1.0/24 dan jaringan 192.168.2.0/24. Pada pengaturan ini disediakan dua *pool* untuk dua jaringan tersebut. Pada *pool* pertama disediakan alamat IP dari 192.168.1.2 sampai dengan 192.168.1.254. Pada *pool* kedua disediakan alamat IP dari 192.168.2.2 sampai dengan 192.168.2.254. Alamat IP 192.168.1.1 dan 192.168.2.1 tidak disediakan untuk komputer klien karena dipakai sebagai alamat IP antarmuka *router*. Dua alamat IP ini masing-masing menjadi alamat *default gateway* untuk dua jaringan yang menjadi tanggung jawab *router* A.

Dua pool tersebut selanjutnya dipakai untuk membentuk *server* DHCP pada *router* A. Perintah untuk membentuk *server* DHCP pada *router* adalah sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server add name=dhcp1 interface=ether2
address-pool=pool1
[admin@MikroTik] > ip dhcp-server add name=dhcp2 interface=ether3
address-pool=pool2
```

Pada saat dibentuk, *server* DHCP dalam keadaan tidak aktif. Untuk mengaktifkan *server* DHCP digunakan perintah berikut.

```
[admin@MikroTik] > ip dhcp-server enable dhcp1
[admin@MikroTik] > ip dhcp-server enable dhcp2
```

Hasil konfigurasi *server* DHCP pada *router* A dapat ditampilkan dengan cara sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server print
Flags: X - disabled, I - invalid
 #   NAME   INTERFACE   RELAY   ADDRESS-POOL  LEASE-TIME ADD-ARP
 0   dhcp1  ether2              pool1         3d
 1   dhcp2  ether3              pool2         3d
```

Pada masing-masing jaringan perlu ditetapkan alamat *deafult gateway* dan alamat IP *server* DNS. Untuk menetapkan dua parameter jaringan pada dua alamat jaringan tersebut dilakukan dengan cara sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server network add
address=192.168.1.0/24 gateway=192.168.1.1 dns-
server=8.8.8.8,8.8.4.4
[admin@MikroTik] > ip dhcp-server network add
address=192.168.2.0/24 gateway=192.168.2.1 dns-
server=8.8.8.8,8.8.4.4
```

Hasil pengaturan alamat *default gateway* dan alamat *server* DNS dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server network print
 # ADDRESS         GATEWAY      DNS-SERVER   WINS-SERVER  DOMAIN
 0 192.168.1.0/24  192.168.1.1  8.8.8.8
                                8.8.4.4
 1 192.168.2.0/24  192.168.2.1  8.8.8.8
                                8.8.4.4
```

Dapat dilihat dari tampilan tersebut, pada jaringan 192.168.1.0/24 ditetapkan alamat *default gateway* pada 192.168.1.1. Pada jaringan

192.168.2.0/24 ditetapkan punya alamat *default gateway* pada 192.168.2.1. Pada dua jaringan tersebut ditetapkan alamat *server* DNS pada 8.8.8.8 dan 8.8.4.4. Alamat *server* DNS tersebut adalah *server* DNS Google. *Server* DNS Google dipilih karena dikenal stabil.

Pada jaringan A terdapat dua komputer klien yaitu PC1 dan PC2. Alamat IP pada masing-masing komputer dikonfigurasi dari *server* DHCP yang dijalankan pada *router* A. Dengan demikian, masing-masing komputer klien berlaku sebagai klien DHCP.

Hasil konfigurasi alamat IP pada komputer klien dapat dilihat menggunakan perintah ifconfig dari *shell*. Berikut ini hasil konfigurasi alamat IP pada PC1.

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5A:69:34
          inet addr:192.168.1.2  Bcast:192.168.1.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:274 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26036 (25.4 KiB)  TX bytes:23789 (23.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Komputer PC1 mendapatkan alamat IP 192.168.1.2 netmask 255.255.255.0. Dengan demikian komputer PC1 berhasil mendapatkan alamat IP dari *server* DHCP dengan betul. Pada PC2 juga dapat dibuktikan memperoleh

alamat IP sesuai pengaturan pada *server*.

Konfigurasi lain yang diperoleh dari *server* DHCP adalah *default gateway*. Hasil konfigurasi *default gateway* dapat dilihat menggunakan perintah route. Komputer PC1 memperoleh *default gateway* pada alamat 192.168.1.1 sesuai pengaturan dari *server* DHCP.

Konfigurasi lain yang diatur dari *server* DHCP adalah alamat IP *server* DNS. Konfigurasi *server* DNS dapat dilihat pada *file* /etc/resolv.conf. Isi *file* resolv.conf yang dihasilkan adalah sebagai berikut.

```
# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Alamat IP *server* DNS yang diperoleh komputer PC1 Adalah 8.8.8.8 dan 8.8.4.4 sesuai dengan yang ditentukan dalam *server* DHCP. Dengan demikian, komputer PC1 berhasil memperoleh alamat *server* DNS sesuai pengaturan pada *server* DHCP.

Sampai pada tahap ini, komputer pada jaringan A sudah dapat terhubung dengan jaringan Internet. Untuk membuktikan bahwa komputer klien sudah dapat terhubung dengan jaringan Internet, dilakukan uji ping. Berikut ditampilkan uji ping dari komputer PC1 terhadap *server* Google.

```
# ping www.google.com
PING www.google.com (173.194.38.148): 56 data bytes
64 bytes from 173.194.38.148: seq=0 ttl=49 time=129.139 ms
64 bytes from 173.194.38.148: seq=1 ttl=49 time=150.647 ms
64 bytes from 173.194.38.148: seq=2 ttl=49 time=161.469 ms
64 bytes from 173.194.38.148: seq=3 ttl=49 time=146.877 ms
^C
--- www.google.com ping statistics ---
```

```
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 129.139/147.033/161.469 ms
```

Hasil uji ping menunjukkan bahwa komputer PC1 sudah berhasil terhubung dengan jaringan Internet. Hasil yang serupa juga dapat ditunjukkan dari komputer PC2.

Dengan demikian, konfigurasi jaringan A untuk menghubungkan pada jaringan Internet sudah selesai. Hal demikian menjadi syarat awal untuk penerapan VPN PPTP untuk integrasi dua jaringan.

Pengaturan Pada Jaringan B

Langkah-langkah yang sama harus dilakukan pada jaringan B. Konfigurasi awal yang dilakukan adalah pada *router* B yang meliputi alamat IP dan NAT. Antarmuka pada *router* B ada tiga yaitu ether1, ether2 dan ether3. Antarmuka ether1 merupakan antarmuka *router* yang menghadap jaringan publik. Alamat IP antarmuka ether1 mengikuti alamat IP yang diberikan oleh jaringan laboratorium menggunakan protokol DHCP. Dengan demikian antarmuka ether1 dikonfigurasi sebagai klien DHCP. Alamat IP pada antarmuka ether2 dan ether3 diatur secara manual sesuai jaringan yang dilayani. Pengaturan alamat IP pada seluruh antarmuka pada *router* B dilakukan dengan beberapa perintah berikut.

```
[admin@MikroTik] > ip dhcp-client add interface=ether1
[admin@MikroTik] > ip dhcp-client enable ether1
[admin@MikroTik] > ip address add interface=ether2
address=192.168.11.1/24
[admin@MikroTik] > ip address add interface=ether3
address=192.168.22.1/24
```

Hasil konfigurasi alamat IP antarmuka pada *router* A dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 172.18.105.101/26  172.18.105.64   ether1
 1   192.168.11.1/24    192.168.11.0    ether2
 2   192.168.22.1/24    192.168.22.0    ether3
```

Alamat IP yang diperoleh antarmuka ether1 dari *server* DHCP laboratorium Periferal STMIK AKAKOM adalah 172.18.105.101/26. Alamat IP ini merupakan alamat IP dinamis. Dalam percobaan tingkat laboratorium diperlakukan seperti alamat IP publik. Antarmuka ether2 dan ether3 diberi alamat IP yang satu jaringan dengan jaringan yang menjadi tanggung jawabnya. Antarmuka ether2 diberi alamat IP 192.168.11.1/24, sedangkan antarmuka ether2 diberi alamat IP 192.168.22.1/24.

Tabel *routing* yang berkaitan dengan jaringan yang menjadi tanggung jawab *router* secara otomatis akan dibentuk oleh *router*. Tabel *routing* yang otomatis terbentuk dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.126  1
 1 ADC  172.18.105.64/26  172.18.105.101  ether1          0
 2 ADC  192.168.11.0/24   192.168.11.1    ether2          0
 3 ADC  192.168.22.0/24   192.168.22.1    ether3          0
```

Tabel *routing* yang yang otomatis terbentuk setelah *router* diberi alamat IP diberi kode ADC. *Default route* pada *router* B adalah 172.18.105.126 yang

diperoleh secara otomatis dari *router* laboratorium.

Pada *router* B juga dikonfigurasi aturan yang berkaitan dengan rantai NAT. *Router* menjalankan fungsi sebagai *Firewall*. Mesin *Firewall* melakukan proses NAT terhadap paket data yang berasal dari jaringan 192.168.11.0/24 dan jaringan 192.168.22.0/24. Di sini juga digunakan salah satu bentuk NAT yang disebut *masquerade*.

```
[admin@MikroTik] > ip firewall nat add chain=srcnat
action=masquerade out-interface=ether1 src-
address=192.168.11.0/24
[admin@MikroTik] > ip firewall nat add chain=srcnat
action=masquerade out-interface=ether1 src-
address=192.168.22.0/24
```

Hasil konfigurasi aturan rantai *Firewall* yang diterapkan pada *router* B dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=srcnat action=masquerade src-address=192.168.11.0/24
out-interface=ether1

 1   chain=srcnat action=masquerade src-address=192.168.22.0/24
out-interface=ether1
```

Aturan rantai *Firewall* pertama menunjukkan bahwa paket data yang berasal dari jaringan 192.168.11.0/24 yang keluar melalui antarmuka ether1 dikenakan proses *masquerade*. Aturan kedua menunjukkan bahwa paket data yang berasal dari jaringan 192.168.22.0/24 yang keluar melalui antarmuka ether1 dikenakan proses *masquerade*.

Router B berlaku juga sebagai *server* DHCP untuk melayani permintaan

alamat IP, *default gateway* dan *server* DNS pada komputer klien. Pengaturan pertama *server* DHCP pada *router* B adalah pengaturan *pool* alamat IP yang akan diberikan kepada komputer klien. Pengaturan *pool* alamat IP komputer klien dapat dilakukan sebagai berikut.

```
[admin@MikroTik] > ip pool add name=pool1 ranges=192.168.11.2-
192.168.11.254
[admin@MikroTik] > ip pool add name=pool2 ranges=192.168.22.2-
192.168.22.254
```

Hasil pengaturan *pool* alamat IP dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip pool print
 # NAME                    RANGES
 0 pool1                   192.168.11.2-192.168.11.254
 1 pool2                   192.168.22.2-192.168.22.254
```

Router B punya tanggung jawab untuk mengelola dua jaringan yaitu jaringan 192.168.11.0/24 dan jaringan 192.168.22.0/24. *Pool* pertama disediakan alamat IP dari 192.168.11.2 sampai dengan 192.168.11.254. *Pool* kedua disediakan alamat IP dari 192.168.22.2 sampai dengan 192.168.22.254. Alamat IP 192.168.11.1 dan 192.168.22.1 tidak disediakan untuk komputer klien karena dipakai sebagai alamat IP antarmuka *router*. Dua alamat IP ini masing-masing menjadi alamat *default gateway* untuk dua jaringan yang menjadi tanggung jawab *router* B.

Dua pool tersebut dipakai untuk membentuk *server* DHCP pada *router* B. Perintah untuk membentuk *server* DHCP pada *router* adalah sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server add name=dhcp1 interface=ether2
address-pool=pool1
```

```
[admin@MikroTik] > ip dhcp-server add name=dhcp2 interface=ether3
address-pool=pool2
```

Server DHCP yang terbentuk, perlu diaktifkan menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server enable dhcp1
[admin@MikroTik] > ip dhcp-server enable dhcp2
```

Hasil konfigurasi *server* DHCP pada *router* A dapat ditampilkan dengan cara sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server print
Flags: X - disabled, I - invalid
 #   NAME   INTERFACE   RELAY   ADDRESS-POOL  LEASE-TIME ADD-ARP
 0   dhcp1  ether2              pool1         3d
 1   dhcp2  ether3              pool2         3d
```

Pengaturan *server* DHCP selanjutnya adalah penetapan alamat *default gateway* dan alamat IP *server* DNS. Untuk menetapkan dua parameter jaringan pada dua alamat jaringan tersebut dilakukan dengan cara sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server network add
address=192.168.11.0/24 gateway=192.168.11.1 dns-
server=8.8.8.8,8.8.4.4
[admin@MikroTik] > ip dhcp-server network add
address=192.168.22.0/24 gateway=192.168.22.1 dns-
server=8.8.8.8,8.8.4.4
```

Hasil pengaturan alamat *default gateway* dan alamat *server* DNS dapat ditampilkan sebagai berikut.

```
[admin@MikroTik] > ip dhcp-server network print
 # ADDRES           GATEWAY       DNS-SERVER  WINS-SERVER  DOMAIN
 0 192.168.11.0/24  192.168.11.1  8.8.8.8
                                  8.8.4.4
 1 192.168.22.0/24  192.168.22.1  8.8.8.8
```

```
8.8.4.4
```

Hasil tampilan tersebut menunjukkan bahwa pada jaringan 192.168.11.0/24 ditetapkan alamat *default gateway* pada 192.168.11.1. Pada jaringan 192.168.22.0/24 ditetapkan alamat *default gateway* pada 192.168.22.1. Pada dua jaringan tersebut ditetapkan alamat *server* DNS pada 8.8.8.8 dan 8.8.4.4.

Jaringan B terdapat dua komputer klien yaitu PC3 dan PC4. Alamat IP pada masing-masing komputer dikonfigurasi dari *server* DHCP yang dijalankan pada *router* A. Hasil konfigurasi alamat IP pada komputer klien dapat dilihat menggunakan perintah ifconfig. Berikut ini hasil konfigurasi alamat IP pada PC3.

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A8:65:DB
          inet addr:192.168.11.2  Bcast:192.168.11.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4872 (4.7 KiB)  TX bytes:3745 (3.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Komputer PC3 mendapatkan alamat IP 192.168.11.2 netmask 255.255.255.0. Dengan demikian komputer PC1 berhasil mendapatkan alamat IP dari *server* DHCP dengan betul. Pada PC4 juga dapat dibuktikan memperoleh alamat IP sesuai pengaturan pada *server*. Dengan cara yang sama dengan yang diberlakukan pada PC1, *default gateway* pada PC3 adalah 192.168.1.1. Alamat

server DNS sebagai acuan pada jaringan B sama dengan jaringan A yaitu 8.8.8.8 dan 8.8.4.4.

Sampai pada tahap ini, komputer pada jaringan B sudah dapat terhubung dengan jaringan Internet. Untuk membuktikan bahwa komputer klien sudah dapat terhubung dengan jaringan Internet, dilakukan uji ping. Berikut ditampilkan uji ping dari komputer PC1 terhadap *server* Google.

```
# ping www.google.com
PING www.google.com (173.194.38.146): 56 data bytes
64 bytes from 173.194.38.146: seq=0 ttl=49 time=258.880 ms
64 bytes from 173.194.38.146: seq=1 ttl=49 time=225.220 ms
64 bytes from 173.194.38.146: seq=2 ttl=49 time=139.862 ms
64 bytes from 173.194.38.146: seq=3 ttl=49 time=176.641 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 139.862/200.150/258.880 ms
```

Hasil uji ping menunjukkan bahwa komputer PC3 sudah berhasil terhubung dengan jaringan Internet. Hasil yang serupa juga dapat ditunjukkan dari komputer PC4. Dengan demikian, konfigurasi jaringan B untuk menghubungkan pada jaringan Internet sudah selesai.

Menghubungkan *Router* A dan *Router* B

Langkah berikutnya untuk mengintegrasikan dua jaringan yang terpisah adalah menghubungkan dua *router* pada jaringan tersebut. Untuk menghubungkan dua *router* digunakan metode VPN PPTP. Implementasi metode ini mengharuskan salah *router* berlaku sebagai *server* PPTP dan yang lain sebagai klien PPTP. Pada penelitian ini, *router* A dijadikan *server* PPTP, sedangkan *router* B sebagai klien

PPTP.

Sebagai *server* PPTP, *router* A harus mempunyai alamat IP publik. *Server* PPTP harus dapat dikenal secara publik. Hal demikian diperlukan karena *server* PPTP nantinya akan dihubungi dari klien PPTP dari mana pun. *Server* PPTP sifatnya pasif menunggu hubungan dari klien PPTP.

Router B sebagai klien PPTP tidak perlu menggunakan IP publik. *Router* B hanya berlaku sebagai klien yang nantinya secara aktif harus menghubungi *server* PPTP. Namun demikian, diizinkan juga klien PPTP menggunakan IP publik. Dalam pengertian ini, yang penting klien PPTP dapat menghubungi *server* PPTP.

Langkah pertama menghubungkan *router* A sebagai dan *router* B adalah melakukan konfigurasi *router* A sebagai *server* PPTP. Mikrotik secara *default* menyediakan fitur *server* PPTP. Fitur ini perlu diaktifkan menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > interface pptp-server server set enabled=yes
```

Hasil konfigurasi *router* A sebagai *server* PPTP dapat ditampilkan menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > interface pptp-server server print
            enabled: yes
            max-mtu: 1460
            max-mru: 1460
               mrru: disabled
    authentication: mschap1,mschap2
  keepalive-timeout: 30
    default-profile: default-encryption
```

Supaya *server* PPTP lebih aman, ditetapkan *username* dan *password* untuk

menghubungi *server*. Untuk menetapkan *username* dan *password* digunakan perintah berikut.

```
[admin@MikroTik] > ppp secret add name="pptp-server01"
service=pptp password="220" local-address=192.168.55.1 remote-
address=192.168.55.2 disabled=no
```

Dengan menggunakan perintah di atas, berarti ditetapkan *username* adalah pptp-server01 dan *password* adalah 220. Pada perintah tersebut juga ditetapkan alamat IP privat yang ditetapkan pada *server* PPTP 192.168.55.1, sedangkan alamat IP privat untuk klien PPTP adalah 192.168.55.2. *Username* ditentukan dengan pengarah *name*, *password* ditentukan dengan pengarah *password*, alamat IP privat *server* PPTP ditentukan dengan pengarah *local-address*, sedangkan alamat IP privat klien PPTP ditentukan dengan pengarah *remote-address*.

Langkah selanjutnya, *router* B dikonfigurasi sebagai klien PPTP. Mikrotik secara *default* mempunyai fitur klien PPTP. Untuk menjalankan klien PPTP, *server* PPTP harus dalam keadaan siap. Apabila *server* PPTP belum siap, maka hubungan PPTP akan mengalami kegagalan. Dengan demikian perlu koordinasi antara *server* dan klien PPTP.

Untuk menjalankan klien PPTP diperlukan beberapa parameter yaitu alamat IP *server* PPTP, *username* dan *password*. Untuk menjalankan klien PPTP digunakan perintah sebagai berikut.

```
[admin@MikroTik] > interface pptp-client add name=pptp-client01
connect-to=172.18.105.61 user="pptp-server01" password="220"
disabled=no
```

Maksud perintah tersebut adalah menjalankan klien PPTP untuk menghubungkan diri pada *server* PPTP yang beralamat di 172.18.105.61 menggunakan *username* pptp-server01 dan *password* 220. Alamat IP yang dipakai dalam percobaan pada tingkat laboratorium masih menggunakan alamat IP privat milik laboratorium. Pada penerapan lapangan, alamat IP ini harus berupa alamat IP publik.

Apabila klien berhasil menghubungi *server* PPTP, maka hasilnya dapat dilihat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > interface pptp-client print
Flags: X - disabled, R - running
 0    name="pptp-client01" max-mtu=1460 max-mru=1460
mrru=disabled
      connect-to=172.18.105.61 user="pptp-server01"
password="220"
      profile=default-encryption add-default-route=no dial-on-
demand=no
      allow=pap,chap,mschap1,mschap2
```

Setelah *server* dan klien PPTP berhasil terhubung, muncul antarmuka baru pada *router* A dan *router* B berkaitan dengan hubungan PPTP. Antarmuka ini punya alamat sesuai pengaturan yang sudah ditetapkan. Pada *server* PPTP (*router* A), konfigurasi alamat IP dapat dilihat dengan perintah sebagai berikut.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 172.18.105.61/26   172.18.105.0    ether1
 1   192.168.1.1/24     192.168.1.0     ether2
 2   192.168.2.1/24     192.168.2.0     ether3
 3 D 192.168.55.1/32    192.168.55.2    <pptp-pptp-server01>
```

Pada *router* A terdapat tambahan antarmuka bernama pptp-pptp-server01.

Antarmuka ini muncul karena adanya hubungan VPN PPTP. Pada tampilan tersebut dapat dilihat, antarmuka ini punya alamat IP 192.168.55.1 sesuai dengan yang ditetapkan.

Selain alamat IP, muncul juga tambahan tabel *routing* berkaitan dengan hubungan VPN PPTP. Isi tabel *routing* pada *router* A dapat dilihat dengan perintah sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.62   1
 1 ADC  172.18.105.0/26   172.18.105.61   ether1          0
 2 ADC  192.168.1.0/24    192.168.1.1     ether2          0
 3 ADC  192.168.2.0/24    192.168.2.1     ether3          0
 4 ADC  192.168.55.2/32   192.168.55.1    <pptp-pptp-... 0
```

Pada hasil tampilan dapat dilihat terdapat tambahan satu rute menuju jaringan 192.168.55.2/32 dengan *flag* ADC. Rute menuju jaringan ini dilewatkan pada antarmuka pptp-pptp-server01. Rute ini berkaitan dengan jaringan yang dipakai untuk menghubungkan dua *router*. Jaringan ini merupakan jaringan *Point-to-Point*.

Pada *router* B juga terdapat tambahan antarmuka berkaitan dengan hubungan VPN PPTP. Konfigurasi alamat IP pada *router* B dapat dilihat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 172.18.105.101/26  172.18.105.64   ether1
 1   192.168.11.1/24    192.168.11.0    ether2
 2   192.168.22.1/24    192.168.22.0    ether3
```

```
 3 D 192.168.55.2/32    192.168.55.1    pptp-client01
```

Pada *router* B terdapat tambahan antarmuka bernama pptp-client01. Antarmuka ini berkaitan dengan hubungan VPN PPTP yang sedang terjadi. Alamat IP antarmuka ini adalah 192.168.55.2 sesuai dengan yang ditetapkan.

Pada *router* B juga terdapat tambahan isi tabel *routing*. Untuk melihat ini tabel *routing* pada *router* B digunakan perintah sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.126  1
 1 ADC  172.18.105.64/26  172.18.105.101  ether1          0
 2 ADC  192.168.11.0/24   192.168.11.1    ether2          0
 3 ADC  192.168.22.0/24   192.168.22.1    ether3          0
 4 ADC  192.168.55.1/32   192.168.55.2    pptp-client01   0
```

Pada tampilan tersebut dapat dilihat isi tabel *routing* secara keseluruhan. Tambahan isi tabel *routing* berkaitan dengan tambahan rute menuju jaringan 192.168.55.1/32. Rute menuju jaringan ini dilewatkan pada antarmuka pptp-client01. Jaringan ini merupakan jaringan *Point-to-Point*.

Sampai pada langkah tersebut, hubungan antara *router* A dan *router* B sudah dapat berjalan menggunakan metode VPN PPTP. Namun demikian, hubungan ini baru terjadi antar *router*. Hubungan antar semua klien anggota jaringan A dan jaringan B belum dapat terjadi. Hal demikian disebabkan jaringan A belum mengenal alamat jaringan semua klien pada jaringan B. Hal yang yang juga terjadi pada jaringan B. Jaringan B belum mengenal alamat jaringan semua klien pada jaringan B.

Alamat jaringan pada jaringan B perlu dikenalkan pada *router* A. sedangkan alamat jaringan pada jaringan A perlu diperkenalkan pada *router* B. Untuk mengenalkan alamat jaringan pada masing-masing jaringan dilakukan dengan menambahkan rute pada tabel *routing*. Pada *router* A perlu ditambahkan rute menggunakan perintah berikut.

```
[admin@MikroTik] > ip route add dst-address=192.168.11.0/24
gateway=192.168.55.2
[admin@MikroTik] > ip route add dst-address=192.168.22.0/24
gateway=192.168.55.2
```

Maksud dua perintah tersebut adalah sebagai berikut. Rute menuju jaringan 192.168.11.0/24 dilewatkan melalui *Gateway* 192.168.55.2. Rute menuju jaringan 192.168.22.0/24 dilewatkan melalui *Gateway* 192.168.55.2. Dua jaringan tersebut adalah anggota pada jaringan B.

Hasil penambahan rute tabel *routing* pada *router* A dapat dilihat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.62   1
 1 ADC  172.18.105.0/26   172.18.105.61   ether1          0
 2 ADC  192.168.1.0/24    192.168.1.1     ether2          0
 3 ADC  192.168.2.0/24    192.168.2.1     ether3          0
 4 A S  192.168.11.0/24                   192.168.55.2    1
 5 A S  192.168.22.0/24                   192.168.55.2    1
 6 ADC  192.168.55.2/32   192.168.55.1    <pptp-pptp-..   0
```

Pada tampilan tersebut dapat dilihat adanya dua tambahan rute pada tabel *routing*. Rute tersebut diberi kode AS (*Active Static*) yang maksudnya rute

tersebut dalam keadaan aktif dan ditambahkan secara statis.

Alamat jaringan pada jaringan A juga perlu dikenalkan pada *router* B. Pada *router* B perlu ditambahkan rute menggunakan perintah berikut.

```
[admin@MikroTik] > ip route add dst-address=192.168.1.0/24
gateway=192.168.55.1
[admin@MikroTik] > ip route add dst-address=192.168.2.0/24
gateway=192.168.55.1
```

Maksud dua perintah tersebut adalah sebagai berikut. Rute menuju jaringan 192.168.1.0/24 dilewatkan melalui *Gateway* 192.168.55.1. Rute menuju jaringan 192.168.2.0/24 dilewatkan melalui *Gateway* 192.168.55.1. Dua jaringan tersebut adalah anggota pada jaringan A.

Hasil penambahan rute tabel *routing* pada *router* B dapat dilihat menggunakan perintah sebagai berikut.

```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS       PREF-SRC        GATEWAY         DISTANCE
 0 ADS  0.0.0.0/0                         172.18.105.126  1
 1 ADC  172.18.105.64/26  172.18.105.101  ether1          0
 2 A S  192.168.1.0/24                    192.168.55.1    1
 3 A S  192.168.2.0/24                    192.168.55.1    1
 4 ADC  192.168.11.0/24   192.168.11.1    ether2          0
 5 ADC  192.168.22.0/24   192.168.22.1    ether3          0
 6 ADC  192.168.55.1/32   192.168.55.2    pptp-client01   0
```

Hasil tambahan rute pada tabel *routing* diberi kode AS yang maksudnya rute tersebut dalam keadaan aktif dan ditambahkan secara statis.

Sampai pada tahap ini, integrasi jaringan A dan jaringan B sudah berhasil dilakukan. Untuk menguji secara cepat hasil integrasi dapat dilakukan

menggunakan uji ping. Uji ping diterapkan menggunakan alamat IP privat yang diterapkan pada jaringan A maupun jaringan B.

Berikut ini ditampilkan hasil uji ping dari klien PC1 pada jaringan A menuju klien PC3 dan PC4 pada jaringan B.

```
# ping 192.168.11.2
PING 192.168.11.2 (192.168.11.2): 56 data bytes
64 bytes from 192.168.11.2: seq=0 ttl=62 time=23.439 ms
64 bytes from 192.168.11.2: seq=1 ttl=62 time=4.672 ms
64 bytes from 192.168.11.2: seq=2 ttl=62 time=4.553 ms
64 bytes from 192.168.11.2: seq=3 ttl=62 time=4.831 ms
^C
--- 192.168.11.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.553/9.373/23.439 ms

# ping 192.168.22.2
PING 192.168.22.2 (192.168.22.2): 56 data bytes
64 bytes from 192.168.22.2: seq=0 ttl=62 time=31.733 ms
64 bytes from 192.168.22.2: seq=1 ttl=62 time=4.675 ms
64 bytes from 192.168.22.2: seq=2 ttl=62 time=10.360 ms
64 bytes from 192.168.22.2: seq=3 ttl=62 time=4.351 ms
^C
--- 192.168.22.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.351/12.779/31.733 ms
```

Hasil uji ping menunjukkan bahwa PC1 sudah dapat terhubung dengan PC3 dan PC4. Hasil yang sama juga dapat dibuktikan hasil uji ping dati PC2 menuju PC3 dan PC4.

Dengan demikian, pada tingkat laboratorium integrasi dua jaringan sudah berhasil dilakukan. Konfigurasi untuk integrasi jaringan A dan jaringan B merupakan konfigurasi dasar. Selanjutnya konfigurasi ini dipakai di lapangan dengan beberapa perubahan.

5.1.2 Implementasi Pada Lapangan

Konfigurasi yang sudah ditetapkan di laboratorium dapat langsung diterapkan di lapangan dengan beberapa perubahan. Beberapa perubahan yang dilakukan ketika diterapkan di lapangan adalah sebagai berikut.

- Pemberian alamat IP pada *router* dilakukan secara statis. Pada implementasi laboratorium, antarmuka yang menghadap jaringan publik diberi alamat IP secara dinamis. Pada implementasi lapangan semua antarmuka diberi alamat IP secara statis. Pemberian alamat IP secara statis dilakukan baik pada *router* PP putra maupun putri.
- Penambahan pool alamat IP sesuai dengan kebutuhan *sub network*. Pada implementasi laboratorium, yang dilayani oleh masing-masing *router* hanya dua jaringan. Pada implementasi lapangan, *router* PP Putra melayani empat jaringan, sedangkan *router* PP Putri melayani tiga jaringan. Pada pondok pesantren putra terdapat empat *sub network* yaitu 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 dan 192.168.4.0/24. Pada pondok pesantren putri terdapat tiga *sub network* yaitu 192.168.11.0/24, 192.168.22.0/24 dan 192.168.33.0/24.
- Penambahan aturan rantai *Firewall*. Penambahan ini disebabkan adanya penambahan jumlah sub jaringan. Penambahan ini dilakukan baik pada *Router* PP Putra maupun Putri.
- Penyesuaian alamat IP publik. Penyesuaian alamat IP publik hanya dilakukan pada *router* PP Putra karena *router* ini berlaku sebagai *server* PPTP. Alamat IP publik *router* PP Putra adalah 202.169.226.201/24.

Router PP Putri secara prinsip tidak perlu diubah. Yang perlu dilakukan adalah menyesuaikan alamat IP sesuai provider Internet yang digunakan.

- Penambahan rute pada tabel *routing*. Penambahan rute perlu dilakukan karena penambahan jumlah sub jaringan yang dilayani oleh dua *router* tersebut. Penambahan dilakukan baik untuk *router* PP Putra maupun Putri.
- Perubahan alamat IP target *server* PPTP. Perubahan ini disebabkan alamat IP publik yang ditetapkan pada *server* PPTP mengalami perubahan.

5.2 Pembahasan

Untuk melihat hasil integrasi antara dua jaringan dapat dilakukan menggunakan beberapa cara. Berikut ini dijabarkan beberapa pengaruh yang terjadi setelah berhasil dilakukan proses integrasi jaringan antara jaringan A dan jaringan B..

Alamat IP pada PC yang berbasis pada sistem Linux dapat dilihat menggunakan perintah ifconfig seperti pada implementasi. Alamat IP pada sistem Windows dapat dilihat menggunakan perintah ipconfig. Perintah ini dituliskan pada *prompt* DOS. Berikut ini adalah hasil pemberian alamat IP pada salah satu klien yang menggunakan sistem operasi Windows.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.254
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
        Default Gateway . . . . . . . . . : 192.168.2.1
```

Alamat IP tersebut adalah hasil konfigurasi secara otomatis melalui *server* DHCP yang dijalankan pada *router* A. Alamat IP yang diperoleh termasuk dalam jaringan 192.168.2.0/24 yang menjadi tanggung jawab *router* A. Alamat *default gateway* yang diperoleh adalah 192.168.2.1 yang merupakan alamat IP pada antarmuka *router* A.

Salah satu komputer yang ada pada jaringan B difungsikan sebagai *server* HTTP dan *server* MySQL. *Server* HTTP digunakan untuk melayani permintaan akses terhadap informasi Web. *Server* MySQL digunakan untuk melayani permintaan penyimpanan data secara terpusat. Dari sudut pandang integrasi jaringan, dua *server* tersebut disebut dengan *server*. Pada penelitian ini tidak diteliti lebih lanjut perubahan mekanisme pelayanan terhadap dua *server* dari akses lokal. Penelitian hanya menggambarkan perubahan mendasar pada cara akses terhadap dua *server* tersebut dari akses lokal dilihat dari sudut pandang integrasi jaringan.

Server diletakkan pada jaringan B yang berarti berada pada pondok pesantren putri. Alamat IP yang diperoleh oleh *server* dapat diperoleh menggunakan perintah berikut.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.22.254
```

```
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.22.1
```

Alamat IP yang diperoleh *server* adalah 192.168.22.254 yang merupakan alamat IP hasil konfigurasi otomatis oleh *router* B. Alamat IP *default gateway server* 192.168.22.1 yang merupakan alamat IP salah satu antarmuka *router* B.

Beberapa pengujian yang dilakukan pada penelitian integrasi jaringan ini adalah sebagai berikut.

- Hubungan komputer yang ada pada sistem jaringan terhadap mesin yang berada di luar kedua sistem jaringan.
- Hubungan komputer dengan komputer lain dalam dua sistem jaringan.
- Rute yang dilewati paket data menuju *server* luar.
- Rute yang dilewati paket data dalam dua sistem jaringan.
- *Share* data antara dua sistem jaringan.
- Hubungan komputer dengan *server* HTTP.
- Hubungan komputer dengan *server* MySQL.
- Kecepatan *download*.

Hubungan komputer dalam sistem jaringan dengan *server* di luar sistem jaringan dilakukan dengan uji ping. Uji ping terutama digunakan untuk memastikan bahwa sistem jaringan sudah terhubung pada jaringan Internet. Hal demikian menjadi syarat supaya metode VPN PPTP dapat berjalan. Berikut ini adalah hasil uji ping menuju *server* Google.

```
C:\> ping www.google.com

Pinging www.google.com [173.194.38.176] with 32 bytes of data:

Reply from 173.194.38.176: bytes=32 time=103ms TTL=49
Reply from 173.194.38.176: bytes=32 time=165ms TTL=49
Reply from 173.194.38.176: bytes=32 time=150ms TTL=49
Reply from 173.194.38.176: bytes=32 time=128ms TTL=49

Ping statistics for 173.194.38.176:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 103ms, Maximum = 165ms, Average = 136ms
```

Pada pengujian ini dianggap *server* Google tidak pernah mati. Pemilihan *server* Google disebabkan karena *server* ini terkenal stabil dan dapat dikatakan tidak pernah mengalami mati. Apabila terjadi kegagalan pada uji ini, bukan disebabkan *server* Google yang mati, namun disebabkan jalur menuju *server* terbut yang putus. Hasil uji ping menuju *server* Google menunjukkan bahwa komputer pada sistem jaringan sudah dapat terhubung dengan jaringan Internet. Paket data ICMP yang dikirim menuju *server* Google dapat ditanggapi secara betul. Dengan demikian jalur menuju *server* Google tidak ada yang putus.

Hubungan antar komputer yang berada dalam dua sistem jaringan diuji menggunakan uji ping dari satu komputer pada satu jaringan ke komputer pada jaringan lain. Sebagai contoh, di sini diambil PC2 yang berada pada jaringan A sebagai sumber dan PC4 yang berada pada jaringan B sebagai target. Hasil uji ping antar dua komputer tersebut adalah sebagai berikut.

```
C:\> ping 192.168.22.254

Pinging 192.168.2.254 with 32 bytes of data:

Reply from 192.168.2.254: bytes=32 time<1ms TTL=128
Reply from 192.168.2.254: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.254: bytes=32 time<1ms TTL=128
Reply from 192.168.2.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Sebelum melakukan uji ini, perlu dipastikan terlebih dahulu bahwa PC4 dalam keadaan hidup. Hal demikian perlu dilakukan supaya dapat dipastikan, apabila terjadi kegagalan, maka dipastikan disebabkan hubungan jaringan. Hasil uji ping menunjukkan bahwa PC4 berhasil memberikan tanggapan dari paket ICMP yang dikirim dari PC2.

Dengan uji ping ini diketahui bahwa untuk menghubungi suatu komputer pada suatu jaringan dari komputer pada jaringan lain yang sudah dihubungkan menggunakan metode VPN PPTP, cukup digunakan alamat IP privat. Kondisi ini memungkinkan pengelolaan komputer-komputer pada dua jaringan dikelola secara lokal. Komputer-komputer pada dua jaringan yang sudah dilakukan integrasi dianggap sebagai komputer privat. Komputer-komputer pada jaringan B dianggap sebagai bagian dari jaringan A. Begitu juga sebaliknya, komputer-komputer pada jaringan A dianggap sebagai bagian dari jaringan B.

Rute dari sumber sampai tujuan menggambarkan jumlah *router* yang harus dilewati paket data. Jumlah *router* ini tidak sebanding dengan jarak fisik namun dapat menggambarkan jumlah proses *routing* yang dialami oleh paket data. Semakin banyak melalui suatu *router*, paket data akan semakin mengalami hambatan sampai ke tujuan. Akibat dari hal ini adalah semakin lama waktu yang

diperlukan paket data sampai tujuan. Akibat lain dari banyaknya *router* yang dilalui paket data adalah waktu tanggapan yang semakin besar.

Berikut ini adalah hasil uji terhadap rute yang ditempuh paket data dari komputer PC2 ke *server* Google.

```
C:\> tracert www.google.com

Tracing route to www.google.com [173.194.38.176]
over a maximum of 30 hops:

  1     1 ms     7 ms     1 ms  192.168.2.1
  2    13 ms     1 ms    <1 ms  172.18.105.126
  3     9 ms    <1 ms     6 ms  192.168.1.254
  4    90 ms    94 ms   109 ms  10.20.30.29
  5     *       79 ms     *     10.20.161.2
  6   103 ms    73 ms    82 ms  10.20.161.38
  7     *       90 ms   241 ms  202.70.56.49
  8    86 ms    77 ms    83 ms  202.70.56.17
  9    88 ms    99 ms     *     ip-179-125.moratelindo.co.id
[202.43.179.125]
 10   140 ms   137 ms   129 ms  ip-176-146.moratelindo.co.id
[202.43.176.146]
 11   263 ms   123 ms   131 ms  ip-176-198.moratelindo.co.id
[202.43.176.198]
 12   127 ms   129 ms   122 ms  72.14.210.131
 13   123 ms   113 ms   122 ms  66.249.95.122
 14   131 ms   128 ms   119 ms  72.14.233.105
 15   130 ms   118 ms   118 ms  sin04s02-in-f16.1e100.net
[173.194.38.176]

Trace complete.
```

Uji tracert dari komputer PC2 menuju *server* Google sebetulnya kurang banyak pengaruhnya terhadap hasil Integrasi jaringan. Uji ini menjadi penting apabila hasil uji ping menunjukkan hasil yang mana hubungan putus. Dalam kondisi jaringan putus, uji tracert akan memberikan petunjuk yang mana terjadinya kegagalan. Bisa juga uji tracert menunjukkan pada *router* mana paket data tidak dapat melewati.

Dari hasil uji tracert dapat diketahui bahwa dari komputer PC2 menuju

server Google melalui 14 *router*. Pada beberapa *router* terdapat hasil *. Hal demikian bisa disebabkan oleh beberapa hal. Sebab pertama munculnya tanda * adalah *router* terlalu lama melakukan proses paket data. Sebab lain yang memunculkan tanda * adalah *router* melakukan proteksi terhadap isyarat ICMP. Namun demikian, yang penting adalah paket yang dikirim sampai kepada tujuan.

Uji tracert yang lebih penting lagi adalah antara komputer pada jaringan A menuju komputer pada jaringan B. Seberapa banyak *router* yang dilewati, menggambarkan proses yang harus dilalui paket data selama dalam perjalanan menuju tujuan. Hal demikian menggambarkan seberapa cepat paket sampai kepada tujuan.

Berikut ini adalah hasil uji tracert dari paket yang berasal dari PC2 pada jaringan A menuju komputer PC4 pada jaringan B.

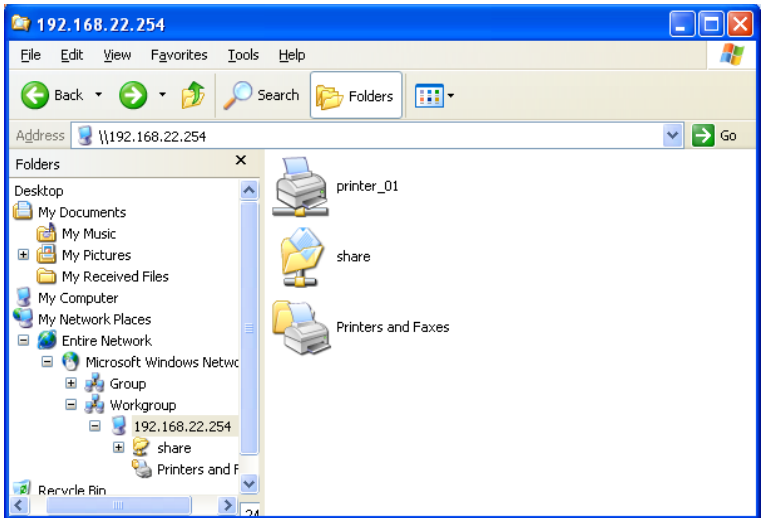
```
C:\> tracert 192.168.22.254

Tracing route to WINXP [192.168.22.254]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  192.168.2.1
  2     2 ms     3 ms     2 ms  192.168.55.2
  3     5 ms     5 ms     5 ms  WINXP [192.168.22.254]

Trace complete.
```

Dari hasil uji tracert dapat dilihat bahwa paket data yang berasal dari PC2 menuju PC4 cukup melalui 2 *router*. *Router* pertama punya alamat IP 192.168.2.1 yang merupakan *router* yang mengelola jaringan A. *Router* kedua punya alamat IP 192.168.55.2 yang merupakan *router* yang mengelola jaringan B. Hal demikian merupakan hasil yang diinginkan dari proses integrasi jaringan. Proses integrasi

jaringan harusnya memperpendek rute yang harus ditempuh paket data dari sumber ke tujuan.

Dari sisi rute, integrasi jaringan menggunakan metode VPN PPTP berhasil memperkecil jumlah *router* yang dilewati oleh paket data. Rute yang sebetulnya harus melalui jaringan publik, dapat disembunyikan sedemikian, sehingga seperti hanya melalui jaringan privat.

Selanjutnya hasil integrasi jaringan diuji dengan melihat pengaruhnya terhadap beberapa layanan yang berjalan di atas jaringan. Layanan pertama yang dilihat pada penelitian adalah s*hare*.



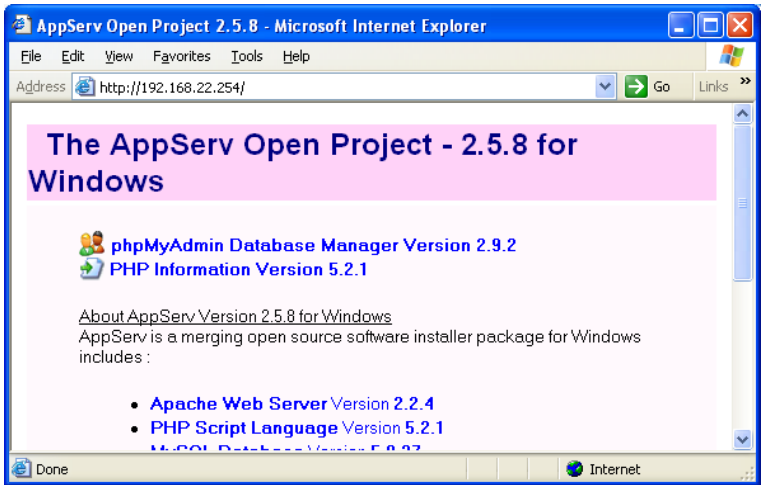
Gambar 5.1 *Share* Data dan Printer

Setelah integrasi jaringan sudah dilakukan, proses *share* antar komputer pada dua sistem jaringan dapat dilakukan. Proses *share* dapat dilakukan pada *file*, direktori, *printer* atau sumber daya jaringan lain. Proses *share* sangat diperlukan

ketika diinginkan untuk menggunakan suatu sumber daya yang terletak pada komputer lain. Proses *share* tidak bisa dilakukan atau sulit dilakukan apabila pada sistem jaringan publik. Kemungkinan beberapa *port* yang dipakai untuk *share* diblok oleh pengelola jaringan. Apabila *port* untuk *share* tidak diblok, yang menyulitkan pada proses *share* melalui jaringan publik adalah bahwa proses *share* memerlukan *server* Wins

Layanan *server* Wins tidak bisa melintasi sistem jaringan yang melintasi *Firewall*. Biasanya untuk hubungan dengan jaringan Internet diperlukan adanya *Firewall*. Dengan adanya integrasi jaringan menggunakan metode VPN PPTP, mesin *Firewall* diabaikan fungsinya. Dengan demikian integrasi jaringan seperti meniadakan mesin *Firewall*. Akibat selanjutnya adalah layanan *server* Wins dapat berjalan. Pada akhirnya layanan *share* antar komputer dapat dijalankan.

Pengujian hubungan HTTP berkaitan dengan integrasi *server* Web antara jaringan A dan jaringan B. Integrasi jaringan punya dampak pada penyatuan *server* Web yang digunakan menampilkan informasi berkaitan dengan pondok pesantren. Berikut ini ditampilkan hasil integrasi jaringan berkaitan dengan akses *server* Web



Gambar 5.2 Hubungan *Server* Web

Integrasi jaringan punya dampak terhadap akses *server* Web berkaitan dengan cara akses. Akses *server* Web dari dalam lingkungan pondok dapat dilakukan secara privat. Secara isi akses privat tidak terlalu berbeda dengan akses secara publik. Namun demikian akses privat ini menjadi sangat penting apabila digunakan untuk mengakses data privat pondok pesantren. Salah satu akses yang terpengaruh adalah akses menuju *server* Database.

Dengan adanya integrasi jaringan dapat meningkatkan keamanan terhadap akses pada *server* Database. Dengan adanya integrasi jaringan, akses *server* Database dapat dilakukan secara lokal. Akses lokal berpengaruh pada pengaturan izin akses pada *server* Database. Izin akses pada *server* Database dapat dibatasi hanya untuk dua jaringan yang dilakukan integrasi, sedangkan izin akses dari luar lingkungan dua pondok dapat dimatikan.

Berikut ini diberikan salah satu tampilan hasil akses *server* Database

MySQL dari dalam jaringan.

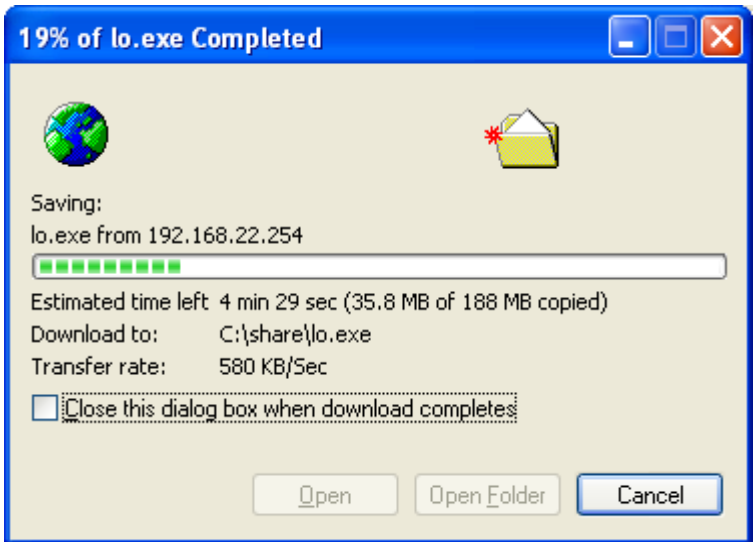
```
C:\> mysql -u user01 -h 192.168.22.254 -p
Enter password: ******
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1 to server version: 5.0.27-
community-nt-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| db_data            |
+--------------------+
2 rows in set (0.02 sec)

mysql> use db_data;
Database changed
mysql> quit
Bye
```

Akses tersebut dilakukan dari salah satu komputer pada jaringan A menuju *server* Database pada jaringan B. *Server* Database punya alamat IP 192.168.22.254. Dalam hal ini akses dilakukan secara langsung tanpa melalui perantaraan *server* Web. Kasus ini terjadi apabila aplikasi dijalankan dari jaringan A, sedangkan *server* Database berada pada jaringan B.

Akses langsung pada *server* Database dari jaringan lain tentunya akan berjalan cukup lambat. Walaupun integrasi sudah dilakukan, namun dari sisi kecepatan tidak akan meningkat. Hal demikian disebabkan hubungan antara dua jaringan masih dilewatkan pada jaringan Internet. Semakin besar *bandwidth* yang disediakan, tentunya akan meningkatkan kecepatan akses pada *server* Database.

Untuk melihat seberapa pengaruh integrasi jaringan terhadap kecepatan, dilakukan uji coba *download file* yang berasal dari jaringan B oleh komputer pada

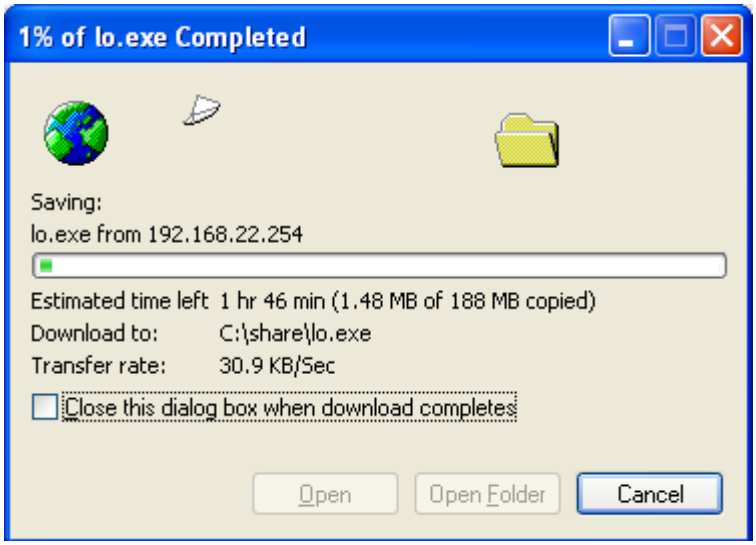
jaringan A. Untuk menguji ini, dicoba dengan membatasi kecepatan *download* untuk *file* yang cukup besar. Berikut hasil uji coba *download* untuk kecepatan tanpa batas.



Gambar 5.3 *Download* Pada Kecepatan Tanpa Batas

Pada kecepatan yang tidak dibatasi, diperoleh kecepatan *download* sebesar 580 KBps. Besar kecepatan ini setara dengan 4640 Kbps. *File* berukuran 188 MB diperkirakan dapat di*download* dalam waktu 4 menit 29 detik. Pengaruh integrasi jaringan mungkin tidak begitu terlihat. Hal ini disebabkan bahwa tidak mungkin membandingkan antara kecepatan tidak terbatas dengan kecepatan yang diperoleh.

Berikut ini ditampilkan hasil *download* pada batas maksimum 256 Kbps untuk *file* yang sama seperti sebelumnya.



Gambar 5.4 *Download* Pada Batas 256 Kbps

Pada hasil tampilan *download* dapat dilihat, kecepatan *download* yang diperoleh adalah 30,9 Kbps atau setara dengan 247,2 Kbps. Kecepatan yang dihasilkan sedikit di bawah nilai batas yang diizinkan yaitu 256 Kbps. *File* berukuran 188 MByte dapat di*download* dalam waktu 1 jam 46 menit. Dengan demikian pengaruh penggunaan VPN PPTP tidak terlalu berpengaruh pada penurunan kecepatan.

BAB 6 KESIMPULAN

6.1 Kesimpulan

Kesimpulan yang dapat diambil dari hasil pembahasan dan percobaan dalam penelitian ini adalah sebagai berikut.

- Prototipe integrasi dua jaringan menggunakan Mikrotik RouterOS™ RB750 pada tingkat laboratorium sudah berhasil dilakukan dan berjalan secara baik.
- Implementasi lapangan prototipe integrasi jaringan pada dua pondok pesantren Ibnul Qoyyim putra dan putri berhasil dilakukan dan berjalan dengan baik.
- Integrasi dua jaringan berhasil memperpendek rute visual yang harus dilewati paket data menuju jaringan yang berbeda.
- Integrasi dua jaringan memudahkan dalam akses sumber daya baik yang berada pada jaringan yang sama maupun jaringan yang berbeda.
- Aplikasi yang sudah diuji hal kemudahan akses setelah integrasi jaringan adalah *share*, HTTP, *server* MySQL, dan *download*.
- Integrasi jaringan jaringan memudahkan akses antar sumber daya dalam jaringan namun sedikit menurunkan proses transfer data.

6.1 Saran

Saran yang diajukan untuk pengembangan dan penelitian lebih lanjut dari penelitian ini adalah sebagai berikut.

- Integrasi jaringan baru bisa diterapkan untuk menyatukan dua jaringan, sehingga perlu dipikirkan pengembangan untuk integrasi banyak jaringan.
- Perlu diteliti lebih lanjut, pengaruh integrasi jaringan menggunakan metode VPN PPTP pada penurunan kecepatan.
- Perlu penelitian lebih lanjut penerapan metode VPN PPTP menggunakan sistem Linux seperti Mandriva, CentOS, dan sebagainya.
- Perlu penelitian lebih lanjut penerapan metode VPN PPTP menggunakan *router* yang punya *processor* lebih baik dari Mikrotik RouterOS™ RB750.

Daftar Pustaka

Angga Wibowo, 2006, *cara mudah membangun LAN, panduan praktis membangun jaringan komputer dalam sehari*, Elex Media Komputindo, Jakarta

Budi Lestari, 2011, *Materi Subnetting*, http://lesta_bd.guru-indonesia.net/artikel_detail-16390.html, 19 April 2012 pkl 21.30 PM

Mikrotik, 2008, *MikroTik RouterOS™ v3.0, Reference Manual*, http://www.mikrotik.com/testdocs/ros/3.0

Mikrotik, 2011, *Router RB750*, http://www.mikrotik.co.id/produk_lihat.php?id=194

Nova Rusdy Setyawan, 2011, *Implementasi VLAN Trunk Protocol(VTP) melalui Ethernet over Internet Protocol (EoIP)Tunnel pada Mikrotik RouterOS*, 17 April 2012 pkl 13.15 AM

Rouse. M., 2005, *Point-to-Point Tunneling Protocol (PPTP)*, http://searchnetworking.techtarget.com/definition/Point-to-Point-Tunneling-Protocol, 16 April 2012 pkl 09.30 AM

Wagito, 2007, *Jaringan Komputer Teori dan Implementasi Berbasis Linux*, GAVA MEDIA Yogyakarta

-------, 2004, EoIP, http:// www.mikrotik.com/testdocs/ros/2.9/interface/eoip.php, 21 Mei 2012 pkl 11.30

------, 2008, Ethernet over IP Tunnel Interface di Mikrotik, http://www.kuebasah.com/ethernet-over-ip-eoip-tunnel-interface-di-mikrotik.html, 17 April 2012

------, 2008, The TCP/IP Stack and OSI Model, http://learn-networking.com/tcp-ip/the-tcpip-stack-and-the-osi-model, 17 Juli 2012 pkl 10.30 AM

------, 2011, Jaringan Berbasis VLAN, http://info. Cakrawala21.com/?p=113, 25 Mei 2012 pkl 09.45.

------, 2011, Pengertian Mikrotik / Mengenal Mikrotik, http: //chapila.com/mikrotik/pengertian-mikrotik-mengenal-mikrotik.html, 16 April 2012 pkl 09.45 AM.

LAMPIRAN

Curriculum Vitae

Nama	: W A G I T O, S.T., M.T.
Umur	: 43 tahun
Pangkat / Golongan	: Pembina Tk 1 / IV B
Jabatan Fungsional	: Lektor Kepala
Riwayat Pendidikan	
SD	: 1983
SMP	: 1986
SMA	: 1989
Sarjana Teknik	: 1994
Magister Teknik	: 1999
Alamat	: Suryoputran Pb III / 44 Yogyakarta 55131